Client Advisory: Office of the Superintendent of Financial Institutions New E-23 Model Risk Management Guidelines

Richard Austin & Amy Ariganello January 6, 2026

On September 11, 2025, the Office of the Superintendent of Financial Institutions ("**OSFI**") released Guideline E-23, *Model Risk Management* (the "**New Guideline**"). The New Guideline sets out OSFI's expectations concerning model risk management by federally regulated financial institutions ("**FRFIs**") and comes into effect on May 1, 2027.

The New Guideline will replace the existing Guideline E-23, *Enterprise-Wide Model Risk Management for Deposit-Taking Institutions* (the "**Existing Guideline**") from 2017 and reflects OSFI's response to the comments it received concerning the draft Guideline E-23 (the "**Draft Guideline**") released in November 2023.

The New Guideline represents a significant change in OSFI's approach to model risk management, the impacts of which extend beyond FRFIs.[1] These changes will affect Suppliers who are providing models within the scope of the New Guideline (referred to as "**captured models**") or providing services incorporating captured models, to these organizations.[2]

Overview

This advisory note is focused on the impacts to those Suppliers, providing them with an overview of the New Guideline and how it may impact them. It is divided into four parts:

(i) **Part I (Introduction)** introduces the New Guideline including details of the expanded scope of organizations to which the New Guideline will apply and the models that will fall within its purview;

(ii) **Part II (Model Lifecycle)** describes OSFI's risk management expectations concerning specific stages of the model lifecycle;

(iii) **Part III (Model Risk Management Framework)** focuses on how the model risk management framework will impact Suppliers; and

(iv) **Part IV (Other OSFI Guidelines)** clarifies the relationship between the New Guideline and other OSFI Guidelines such as Guideline B-10 (Third Party Risk Management) and Guideline B-13 (Technology and Cyber Risk Management).

This advisory is not intended to be a complete statement of the law and does not constitute legal advice. This advisory is for information purposes only.

---

1. Part I – Introduction

Financial institutions' use of models has been increasing in recent years. However, models are only that, a model of reality based on (i) the assumptions underlying the model, (ii) the algorithms

---

[1] Referred to below collectively as "financial institutions" or "organizations".

[2] The New Guideline contains at least 5 references to OSFI's expectations that organizations will apply the New Guideline to models or services incorporating models that are provided by third party suppliers. For example, Section B.2 (Model risk management framework) of the New Guideline sets out the expectation that organizations will establish a MRM framework that will apply to models obtained from external sources.

used, and (iii) the data on which the model is trained. Shortcomings in any of these areas can undermine the reliability and accuracy of the model and create risk for the financial institutions relying on it.

Recognizing the risks to financial institutions arising from the use of models, OSFI released the New Guideline to assist financial institutions in mitigating their model risks by setting out expectations related to enterprise-wide model risk management. The New Guideline follows the format of recent OSFI guidance, and sets out three outcomes that organizations are expected to achieve, based on twelve principles intended to assist organizations in achieving these outcomes.[3] The outcomes that organizations are expected to achieve are:

(i) Model risk is well understood and managed across the enterprise.
(ii) Model risk is managed using a risk-based approach.
(iii) Model governance covers the entire model lifecycle.[4]

A. The Scope of the New Guideline

The scope of the Existing Guideline is limited to the specified deposit taking institutions (i.e., banks**,** bank holding companies, federally regulated trust and loan companies and cooperative retail associations).

In contrast, the New Guideline will apply to all federally regulated financial institutions.[5] This means, for example, that insurance companies will now be included under OSFI's guidance relating to the use of models. Suppliers will need to recognize that other financial institutions in their customer base may be subject to the New Guideline and that these organizations may seek to flow down its requirements to them. One notable exception exists in the coverage as federally regulated pension plans are excluded from the scope of the New Guideline due to the availability of alternative industry guidance addressing risk management.[6]

B. What Models are Covered?

The term "model" is defined in the Existing Guideline, in a manner consistent with the focus of the Existing Guideline on deposit-taking institutions, as:

> "a methodology, system, and/or approach that applies theoretical and (expert) judgmental assumptions and statistical techniques ***to process input data in order to generate quantitative estimates***" (emphasis added).

The New Guideline adopts a broader definition and one that specifically refers to Artificial Intelligence and Machine Learning ("**AI/ML**")[7]:

> "The application of theoretical, empirical, judgmental assumptions and/or statistical techniques, including AI/ML methods ***which processes input data to generate results***."[8] (emphasis added)

---

[3] The expected outcomes and principles are reproduced in Appendix A of this advisory.
[4] Section A.5 of the New Guideline.
[5] Section A.2 of the New Guideline.
[6] Federally regulated pension plans were originally included in the scope of the November 2023 Draft E-23 Guideline but were removed prior to publishing the final New Guideline.
[7] OSFI notes at Footnote 1 of the New Guideline that there are currently no generally agreed definitions of AI/ML. However, for the purposes of the New Guideline, OSFI adopted the OECD definition of "a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."
[8] The New Guideline also refers in its definition of "model" to the three specific components of a model:
1. **data input** component that may also include relevant assumptions.
2. **processing component** that identifies relationships between inputs, and
3. **result component** that presents outputs in a format that is useful and meaningful to business lines and control functions.

This new definition, and OSFI's expectation that under the New Guideline model risk will be managed on an enterprise-wide basis, impacts Suppliers in three ways:

(i) The New Guideline will encompass ***any*** models used by an organization, not just the financial models that are the focus of the Existing Guideline. This means that models provided by Suppliers (e.g., AI screening systems used for HR purposes such as evaluating resumés) or artificial intelligence systems used by Suppliers in providing services to organizations (e.g., screening or ranking customers' loan applications) will fall within the purview of the New Guideline. This appears to be the case even where the AI/ML model has been implemented in the organization on a "human in the loop" basis. The fact that the output generated by the model may be subject to human oversight does not take the model outside the purview of the New Guideline, although it may affect the model's risk rating.

The definition of model in the New Guideline will require Suppliers to review the products and services they and their subcontractors are providing to organizations to determine whether those products or services constitute or involve the supply or use of models (i.e., if they involve "theoretical, empirical, judgmental assumptions or statistical techniques, including AI/ML methods, which process input data to generate results").

This is an assessment that will need to be done initially but, also, on an ongoing basis in connection with any modifications that the Supplier or its subcontractors implement to its or their products or services.

(ii) Under the Existing Guideline, "model risk" is defined in terms of financial and reputational risks. Consistent with the broader scope of its definition of "model", the New Guideline expands the definition of "model risk" to focus on a wide range of adverse financial impacts (e.g., inadequate capital, financial losses, inadequate liquidity, and financial, operational and reputational consequences) arising from flaws or limitations in the design, development, implementation/deployment or use of a model.[9]

(iii) Both the Existing Guideline and the New Guideline refer to proportionality as a factor to be considered by organizations[10] but take different approaches in responding to the issue. The Existing Guideline states explicitly that it applies to "any model that could materially impact the risk profile of an institution",[11] implying that models that do not materially impact the institution's risk profile are out of scope. Under the New Guideline, organizations are required to identify all models carrying **non-negligible inherent model risk**. The effect of identifying a model as carrying a negligible level of inherent model risk, is that it may be exempted from the full model lifecycle governance requirements.[12]

Similar components are identified in the Existing Guideline.

[9] Section A.4 of the New Guideline.

[10] The Existing Guideline states in Section 1 that it should be interpreted in the context of a proportionality principle where applicability is commensurate with the nature, size, complexity and risk profile of the institution. The New Guideline uses slightly different terminology, stating in Section A.3, that the New Guideline applies on a risk-basis proportional to the organizations' size, strategy, risk profile, nature, scope, complexity of operations, and interconnectedness to other financial institutions, the financial system, or the broader economy.

[11] Section 3 of the Existing Guideline.

[12] Section C.2 of the New Guideline.

2. Part II – Model Lifecycle

OSFI expects that organizations will mitigate their model risks by adopting robust risk management practices and oversight and that these practices and oversight will apply throughout the model lifecycle. Indeed, the third outcome that organizations are expected to achieve under the New Guideline is model governance that "covers the entire model lifecycle".[13]

For this to happen, organizations need to have a good understanding of the model lifecycle. OSFI describes the lifecycle in Section D.2 and provides commentary with respect to the different stages of the model lifecycle.

The model lifecycle requirements apply to an individual model based on the assigned model risk ratings. The documentation supporting the model lifecycle is expected to be current, maintained for each phase of the model's lifecycle and commensurate with the risks of the model.

A. Model Design

The New Guideline defines model design, the first stage of the model lifecycle, as encompassing three components, clearly articulating OSFI's expectation that these components will be part of an organization's model lifecycle. The three components that OSFI defines as part of model design are: (i) the establishment of clear organizational rationales for a model, (ii) adherence to standards that ensure data quality and accuracy, and (iii) following appropriate model development processes.[14]

B. Model Rationale

Model owners are expected to be able to identify a clear rationale, whether for deploying a new model or making modifications to an existing one. Based on this provision, Suppliers can anticipate that they will be asked, by their financial institution customers, to justify their use of new models or changes to existing ones. Their rationale will need to encompass, for each model, the specific business use case and the risk of the model's intended usage.[15]

In establishing a rationale for models that use advanced techniques such as AI/ML, model owners should also consider additional factors that arise from the use of these models such as: (i) the level of transparency and explainability required in the rationale, (ii) the need for alternative controls, especially with respect to models that use "black box" approaches or operate autonomously, and (iii) the potential for uses of the model to result in biased outcomes, negative social or ethical implications, or privacy risks.[16]

C. Model Data

This section of the New Guideline sets out the obligations of organizations to ensure that the data used in developing the models satisfies specific criteria and is suitable for its intended use, in line with Principle 3.2.

To align with an organization's responsibilities, Suppliers should be in a position to provide information to their customers about model risks arising from the data used to train the Supplier's models including the measures taken by Suppliers to ensure that the training data is: (i) accurate and fit-for-use; (ii) relevant and representative; (iii) compliant with statutory, regulatory, and internal requirements; (iv) traceable; and (v) timely.[17]

---

[13] Section A.5 of the New Guideline.
[14] Section D.2 of the New Guideline.
[15] *Ibid*.
[16] *Ibid*.
[17] *Ibid*.

The New Guideline also stipulates that financial institutions must consider the potential for bias within data, on the basis that bias can lead to unfair model outputs and reputational risks. Suppliers should perform regular data quality checks, implement controls to ensure data quality, and have controls in place to ensure appropriate data cleansing, as these all may well translate into requirements that Suppliers will need to satisfy in using models as part of their service offerings.

D. Model Development

This section sets out OSFI's expectations for the development processes that will be used by organizations to develop their models and Suppliers can anticipate that these processes will be flowed down to them. These requirements, encompassed in Principle 3.3, involve setting clear standards for performance and documentation and follow what one would expect to see in any industry-standard system development methodology.

Suppliers should review their development methodologies against the requirements of the New Guideline to ensure that they are complying with these requirements and that their compliance is well documented. This may be especially relevant with "learning" models where the algorithms or parameters in use may change over time and where each such change may be subject to the development, validation and approval requirements implemented by organizations in response to the New Guideline.

Financial institutions and Suppliers should establish clear, consistent, and repeatable practices for developing models, which may include: (i) standards for model documentation; (ii) guides on the role of expert judgment; (iii) lists of analyses and performance tests executed by developers; (iv) guides for selecting conceptually sound methodologies, data, and algorithms; (v) explainability requirements; (vi) criteria for model selection; (vii) standards for use and reporting on model outputs; and (viii) criteria for model monitoring.[18]

E. Model Review

Before an organization can approve a model for implementation in production, the model should be validated. The New Guideline suggests validation take place independent of the model development and ensure and document that the model is properly specified, working as intended, and fit for its intended purpose.[19]

These are not "one off" activities. Rather, the extent and frequency of model reviews should be commensurate with the model risk rating. Model validation should be conducted at the development stage, but also when: (i) the models are modified (including in response to internal requirements), (ii) model performance is breached, (iii) the related data is significantly changed, and (iv) on a periodic basis.[20]

---

[18] *Ibid*.
[19] *Ibid*.
[20] The reviewing process may include: (i) confirming or challenging the model risk rating; (ii) reviewing the model purpose, scope, conceptual soundness, limitations, mitigants, and reasonableness of model outcomes; (iii) evaluation of the quality and appropriateness of model data; (iv) reviewing novel methodologies, algorithms, tools, and procedures for AI/ML models; (v) assessments of the explanations provided by the model as to how it produces outcomes; (vi) reviewing third-party models, platforms, and sub-components used in development; (vii) verification that review assessment documentation is complete; and (viii) reporting on the outcome of the reviewing process.

F. Model Approval

The model approval processes should be repeated throughout the lifecycle of a model. A model's approval should involve an assessment of whether the model is or remains suitable to be implemented based on its intended use, and whether the assigned model risk rating is still appropriate.[21] Suppliers should seek to understand model approval requirements at an early stage in the development process in order to respond to these requirements.

G. Model Deployment

Principle 3.5 sets out that models should be deployed in an environment with quality and change control processes. The requirements of the New Guideline relating to model deployment are not unusual but do require:

(i) collaboration among developers, owners, reviewers, users, and technology/operations teams;

(ii) consistency between the data used to develop the model and the production data;

(iii) tests demonstrating that the model operates as expected in the production environment;

(iv) clearly documented procedures for deployment steps, stakeholder responsibilities, approval hierarchies, change control, monitoring frameworks, and exception handling;

(v) performance of risk assessments for cybersecurity, infrastructure vulnerabilities, and other operational risks prior to deployment; and

(vi) review of explainability requirements and communication of explanatory outputs to key stakeholders.[22]

H. Model Monitoring

After a model is deployed, organizations are required to monitor and validate the model on a periodic basis that corresponds with the model's risk rating. To align with the responsibilities of organizations, Suppliers will need to monitor their models and to also validate them on a periodic basis. Model monitoring should document and include:

(i) monitoring standards regarding frequency, scope, and evaluation criteria based on risk rating;

(ii) both quantitative (e.g. performance metrics) and qualitative (e.g., ensuring model is within scope) evaluating criteria;

(iii) tracking and evaluating operational factors such as model performance, model usage, input data, external dependencies, or the characteristics of what is being modelled;

(iv) defining thresholds for breaches and criteria for material model modifications;

(v) determining contingency plans for model unavailability, deterioration in model performance, or outright failure along with the escalation procedures for addressing these;

---

[21] Section D.2 of the New Guideline.
[22] *Ibid*.

(vi) implementing processes for handling AI/ML's challenges, such as autonomous decision making, autonomous re-parametrization, and the elevated potential for model drift; and

(vii) ensuring issues are shared promptly with relevant stakeholders.

I. Model Decommission

The New Guideline recognizes that models may be decommissioned for (i) performance issues, (ii) business, regulatory or strategic reasons, or (iii) obsolete data or methodologies or cost-benefit considerations. The New Guideline recommends organizations establish disciplined processes to deal with model decommissioning to alert stakeholders, maintain relevant documentation, and avoid residual impacts.[23]

3. Part III – Model Risk Management Framework

OSFI expects organizations to mitigate their model risks by adopting robust risk management practices and oversight, including policies, procedures, and controls. Indeed, the second outcome that organizations are expected to achieve under the New Guideline is model risk that is "managed using a risk-based approach".[24]

The table in **Appendix B** summarizes OSFI's expectations concerning the model risk management (MRM) framework to be implemented by organizations and how the resulting MRM frameworks will impact models that Suppliers provide or use in their services.

Because the MRM frameworks will impact the Suppliers' models (e.g., the data that can be used to train the models, the approvals that are necessary and the reporting that must be provided), Suppliers should seek to understand the organization's MRM framework in as much detail as possible.

4. Part IV – Other OSFI Guidelines

As set out above, the New Guideline sweeps in models developed by FRFI's and models provided by Suppliers to the FRFIs or used by Suppliers in providing services to FRFIs. Suppliers who are using or providing these models will need to consider how the New Guideline may impact their deliverables and services both on a standalone basis and also in step with other guidelines issued by OSFI, for example OSFI's Guideline B-10 (*Third-Party Risk Management Guideline*) and Guideline B-13 (*Technology and Cyber Risk Management*).

Guideline B-10 sets out OSFI's expectations about how FRFIs will manage risks related to third-party arrangements, as defined in the guideline.[25] The definition of third-party arrangements in Guideline B-10 captures the agreements or arrangements under which Suppliers provide models to or use models for FRFIs, bringing these arrangements for models within the purview of Guideline B-10[26] and the Third-Party Risk Management Framework ("**TPRMF**") that FRFIs are required to implement under the Guideline for identifying, managing, mitigating, monitoring, and reporting on risks related to working with third parties.[27] This means that, in addition to the documentation that Suppliers may be required to provide to fulfill model governance expectations under the New Guideline relating to model rationale, data, development, review, approval,

---

[23] *Ibid*.
[24] Section C of the New Guideline.
[25] "Third-party arrangement" is defined in Guideline B-10 as "any type of business or strategic arrangement between the FRFI(s) and an entity(ies) or individuals, by contract or otherwise …".
[26] There is a difference in the scope of application of the New Guideline and Guideline B-10 with respect to foreign bank branches and foreign insurance company branches. See Section A.2 (Scope) of the New Guideline and Section A-1 (Purpose and Scope) of Guideline B-10.
[27] Section 1.2 of Guideline B-10.

deployment, monitoring, and decommissioning,[28] Suppliers should be prepared to provide documentation on their compliance with applicable laws, internal controls, information security programs, and the same for their subcontractors, to FRFIs.[29]

Similarly, Guideline B-13 establishes OSFI's expectations related to technology and cyber risk management, as such terms are defined in Guideline B-13.[30] The technology risk defined in Guideline B-13 will capture the model risk that is the subject of the New Guideline[31] which means that Suppliers will also need to consider the impact on them of the Technology and Cyber Risk Management Framework (the "**RMF**") recommended for FRFIs under Guideline B-13.[32] This RMF overlaps with the Model Risk Management Framework required under the New Guideline[33]. For example, a FRFI's RMF is expected to set out the FRFI's appetite for technology and cyber risk and define the FRFI's processes and requirements to identify, assess, manage, monitor and report on technology and cyber risks.[34] However, using very similar terms, the Model Risk Management Framework under the New Guideline is expected to reflect the FRFIs risk appetite for model risk and to define the processes and requirements to identify, assess, manage, monitor and report on model risk.[35]

FRFIs will respond in different ways to the provisions of OSFI guidelines (including the New Guideline) relating to risk management frameworks. Some may establish a single risk model providing a comprehensive framework for managing risk. At other FRFIs, the risk management responsibility may be divided between different business units, resulting in standalone risk management frameworks that are administered by separate business units. The important point for Suppliers providing models to FRFIs, or services that incorporate models, is to expect multiple layers of oversight depending on factors such as the model and technology risk and the criticality of the services or model provided.

Conclusion

If your organization is subject to the New Guideline, or your customers include FRFIs that are subject to the New Guideline, you should become well versed in the changes that may be required with respect to the use of AI/ML models and facilitating risk management.

If you have any questions, please contact a member of our Technology Law Practice Group.

[28] Section D.2 of the New Guideline.
[29] Annex 1 of Guideline B-10.
[30] The term "technology risk", which includes cyber risk, is defined in Guideline B-13 as "the risk arising from the inadequacy, disruption, destruction, failure, damage from unauthorised access, modifications, or malicious use of information technology assets, people or processes that tenable and support business needs and can result in financial loss and/or reputational damage".
[31] See the definition of "model risk" set out in paragraph 1.B(ii).
[32] Section 1.3 of Guideline B-13.
[33] OSFI acknowledges the overlap between Guideline B-13 and other guidance expressly in Section A.4 of Guideline B-13 where OSFI confirms that Guideline B-13 should be read in conjunction with other OSFI Guidance, tools and supervisory communications and guidance issued by other authorities.
[34] Section 1.3 of Guideline B-13.
[35] Section B.2 of the New Guideline.

Appendix A – Guideline E-23 Expected Outcomes and Principles

A. Expected Outcomes

The following are the expected outcomes of effective MRM:

(i) Model risk is well understood and managed across the enterprise.

(ii) Model risk is managed using a risk-based approach.

(iii) Model governance covers the entire model lifecycle.

B. Principles

Principle 1.1: Effective reporting structures and proper resourcing should enable sound model governance.

Principle 1.2: The MRM framework should align risk-taking activities to strategic objectives and risk appetite.

Principle 1.3: Models should be appropriate for their business purposes.

Principle 2.1: Institutions should identify and track all models in use or recently decommissioned.

Principle 2.2: Institutions should establish a model risk rating approach that assesses key dimensions of model risk.

Principle 2.3: The scope, scale, and intensity of MRM should be commensurate with the risk introduced by the model.

Principle 3.1: MRM policies, procedures, and controls should be robust, flexible, and lead to effective requirements applied across the model lifecycle.

Principle 3.2: Data used to develop the model should be suitable for the intended use.

Principle 3.3: Institutions should have model development processes that set clear standards for performance and documentation.

Principle 3.4: Institutions should have a process to independently assess conceptual soundness and performance of models.

Principle 3.5: Models should be deployed in an environment with quality and change control processes.

Principle 3.6: Institutions should have defined standards for model monitoring, and model decommission.

Appendix B – Supplier Impacts of the Model Risk Management Framework

	Model Risk Management Framework	Supplier Impact
C.	The organization should establish an MRM framework that sets requirements proportional to its exposure to model risk. Organizations should identify sources of model risk, the organization's appetite for model risk, and ensure adequate resources are allocated to manage, mitigate, or accept those risks as appropriate (Outcome 2).	The MRM framework and the organizational appetite for risk that it reflects will determine, for the Supplier's models: (i) the process for and requirements applicable during each stage of the model lifecycle including for approval of models or model changes; and (ii) required reporting.
C.1	The organization should identify and track all models deemed to carry non-negligible inherent model risk and maintain a centralized inventory of models in use and recently decommissioned that includes the information in Appendix A of the New Guideline. The inventory should be comprehensive, evergreen, subject to robust controls and updated in a timely fashion (Principle 2.1).	The Supplier should identify the models (as defined in the New Guideline) it is providing to the organization or using in providing services for the organization. The Supplier will be required to provide information about its models to include in the organization's model inventory and to update this information throughout the model lifecycle in accordance with the organization's requirements.
C.2	The organization's risk rating approach should assess key dimensions of model risk, consider qualitative and quantitative criteria and impacts to downstream processes, and establish remediation actions where models fall outside the institution's risk appetite (Principle 2.2).	The organization's risk rating scheme will determine the level of approval required for the Supplier's model and any updates. It may also impact the frequency of ongoing reviews. The Supplier should seek to understand the organization's risk rating scheme.
	The organization will have an MRM framework that applies to models acquired from an external source.	The MRM framework implemented by the organization for external models will specify the documentation the Supplier is required to provide concerning the design, calibration and operation of its models.
C.3	The organization is expected to develop, as part of its MRM framework, policies, processes, procedures and governing authorities for each phase of the model lifecycle based on the inherent model risk rating (Principle 2.3).	See Item C above.
	The organization's policies should define limits or constraints on model usage, intensity of monitoring, and controls and mitigants to manage residual risk, as aligned with the organization's risk appetite.	The Supplier will need to understand the organization's policies to ensure they are incorporated into the operations of its models. The Supplier should also understand the circumstances in which use of its models could be limited or prohibited and the consequences thereof.
	The organization should determine the inherent model risk rating for each applicable model. The inherent model risk rating should influence: (i) the frequency, intensity and scope of model review, (ii) documentation requirements, (iii) the level of authority required to approve the model, (iv) the frequency, intensity and scope of model monitoring, and (v) the intervals after which the risk rating is reassessed.	The Supplier's models should incorporate the metrics required by the organization's MRM framework and its model procedures should be set up to provide the reporting required by the organization.